

RECEIVED
CENTRAL FAX CENTER

AUG 05 2005

MYERS BIGEL SIBLEY & SAJOVEC, P.A.
Patent Attorneys
4140 Parklake Avenue, Suite 600
P.O. Box 37428
Raleigh, NC 27627
919-854-1400
Facsimile 919-854-1401

**TELECOPIER TRANSMISSION
COVER SHEET**

Date: August 5, 2005 **File Number:** 5577-306
Serial No.: 09/764,844

Telecopier No.: 571-273-8300 **Telephone No.:**

To: Mail Stop Appeal Brief-Patents
Commissioner for Patents

Company: U.S. Patent and Trademark Office

From: Elizabeth A. Stanek, Esq.

Number of Pages: 36 **Return fax to:** Traci

If there is a problem with this transmission, please call (919) 854-1400. Our fax number is (919) 854-1401.

Confidentiality Note

The information contained in this facsimile message is legally privileged and confidential information intended only for the use of the individual or entity named above. If you have received this telecopy in error, please immediately notify us by telephone and return the original message to us at the address above via the United States Postal Service. THANK YOU.

Attorney's Docket No. 5577-306 (RSW920010007US1)

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Doyle *et al.*

Serial No.: 09/764,844

Filed: January 17, 2001

For: SMART CARD WITH INTEGRATED BIOMETRIC SENSOR

Confirmation No.: 6508

Group No.: 2136

Examiner: Carl G. Colin

RECEIVED

CENTRAL FAX CENTER

AUG 05 2005

Date: August 5, 2005

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Facsimile Transmission
I hereby certify that this correspondence is being transmitted
by facsimile to the U.S. Patent and Trademark Office on
August 5, 2005 via facsimile number 571-273-8300.



Traci A. Brown

APPELLANTS' BRIEF ON APPEAL UNDER 37 C.F.R. §41.37

Sir:

This Appeal Brief is filed pursuant to the "Notice of Appeal to the Board of Patent Appeals and Interferences" mailed May 2, 2005.

Real Party In Interest

The real party in interest is assignee International Business Machines Corporation, Armonk, New York.

Related Appeals and Interferences

Appellants are aware of no appeals or interferences that would be affected by the present appeal.

Status of Claims

Appellants appeal the final rejection of Claims 1, 3-23, 33, 35-56 and 58-78, which as of the filing date of this Brief remain under consideration. The attached Appendix A presents the claims at issue as finally rejected in the Final Office Action of March 2, 2005 (hereinafter "Final Office Action") and the Advisory Action of May 26, 2005 (hereinafter "Advisory Action").

Attorney's Docket No. 5577-306 (RSW920010007US1)
In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001
Page 2 of 30

Status of Amendments

The attached Appendix A presents the pending claims and each of the pending claims corresponding status. All amendments in the present case have been entered.

Summary of the Claimed Subject Matter

The present application includes Independent Claims 1, 33 and 56. The claims are system, computer program product and method claims, respectively. Claim 1 is directed to systems for securely providing biometric input from a user. Such systems may be provided by a security component which provides security functions, such that the security component can vouch for authenticity of one or more other components with which the security component is securely operably connected. *See Specification, page 10, lines 7-9.* A biometric sensor component is provided that is securely operably connected, as one of the one or more other components, to the security component. *See Specification, page 10, line 7.* A card containing stored secrets and stored identifying information pertaining to an authorized holder of the card is also provided. *See Specification, page 10, lines 9-10.* A card reader is provided for repeatedly accessing the stored secrets and stored identifying information. *See Specification, page 10, line 11.* The stored identifying information may include stored biometric information of the authorized holder. *See Specification, page 17, lines 11-16.* The card reader is configured to repeatedly access the stored secrets and stored identifying information upon beginning a security-sensitive operation and to terminate repeatedly accessing upon completion of the security-sensitive operation. *See Specification, page 32, line 17 to page 33, line 13.* Means for operably inserting the card into the card reader are also provided. Structure corresponding to the means recitations found in Claim 1 is provided, *inter alia*, by a validation process performed either by the biometric sensor 410 itself or by the security core 150 after securely transferring or accessing the information from the user's smart card.. *See Specification, page 32, line 17 to page 33, line 13 and Figure 4.* Means for establishing a secure, operable connection between the biometric sensor, the card reader, and the security component are also provided. Structure corresponding to the means recitations found in Claim 1 is provided, *inter alia*, by a bus 140 and

Attorney's Docket No. 5577-306 (RSW920010007US1)
In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001
Page 3 of 30

associated processor(s). *See Specification*, page 32, line 17 to page 33, line 13 and Figure 4. Means for comparing the repeatedly obtained biometric information to the stored biometric information of the authorized holder of the card are also provided. Structure corresponding to the means recitations found in Claim 1 is provided, *inter alia*, by a validation process performed either by the biometric sensor 410 itself or by the security core 150 after securely transferring or accessing the information from the user's smart card. *See Specification*, page 32, line 17 to page 33, line 13 and Figure 4. Finally, means for concluding, within the security component, that the security-sensitive operation is authentic based on all the one or more other components which are securely operably connected to the security component remaining securely operably connected to the security component until completion of the security-sensitive operation. Structure corresponding to the means recitations found in Claim 1 is provided, *inter alia*, by a validation process performed either by the biometric sensor 410 itself or by the security core 150 after securely transferring or accessing the information from the user's smart card. *See Specification*, page 32, line 17 to page 33, line 13 and Figure 4.

Independent Claims 33 and 56 are computer program product and method claims corresponding to Claim 1.

Grounds of Rejection to Be Reviewed on Appeal

1. Claims 1, 3-4, 6-7, 10, 13-14, 16-17, 19, 33, 35-36, 38, 39, 42, 45-46, 48-49, 51, 56-59, 61-62, 65, 68-69, 71-72 and 74 stand rejected under 35 U.S.C. §103(a) as being unpatentable over United States Patent No. 6,125,192 to Bjorn *et al.*(hereinafter "Bjorn") in view of United States Patent No. 5,229,764 to Matchett *et al.* (hereinafter "Matchett").

2. Claims 5, 8-9, 11-12, 15, 18, 20-23, 37, 40-41, 43-44, 47, 50, 52-55, 60, 63-64, 66-67, 70, 73 and 75-78 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Bjorn in view of Matchett and in further view of United States Patent No. 6,330,670 to England *et al.* (hereinafter "England").

3. Claims 1, 33, 56 and 69 have been provisionally rejected under the

Attorney's Docket No. 5577-306 (RSW920010007US1)

In re: Doyle *et al.*

Serial No.: 09/764,844

Filed: January 17, 2001

Page 4 of 30

nonstatutory judicially created doctrine of obviousness-type double patenting over copending U.S. Application Serial No. 09/764,827.

Attorney's Docket No. 5577-306 (RSW920010007US1)
In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001
Page 5 of 30

Argument

I. Introduction

The pending claims are rejected as obvious under 35 U.S.C. § 103. To establish a prima facie case of obviousness, the prior art reference or references when combined must teach or suggest *all* the recitations of the claims, and there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. M.P.E.P. §2143. The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. M.P.E.P. §2143.01, citing *In re Mills*, 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1990). As emphasized by the Court of Appeals for the Federal Circuit, to support combining references, evidence of a suggestion, teaching, or motivation to combine must be **clear and particular**, and this requirement for clear and particular evidence is not met by broad and conclusory statements about the teachings of references. *In re Dembiczak*, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999). The Court of Appeals for the Federal Circuit has further stated that, to support combining or modifying references, there must be **particular** evidence from the prior art as to the reason the skilled artisan, with no knowledge of the claimed invention, would have selected these components for combination in the manner claimed. *In re Kotzab*, 55 U.S.P.Q.2d 1313, 1317 (Fed. Cir. 2000).

Appellants respectfully submit that the pending claims are patentable over the cited references because the cited references fail to disclose or suggest the recitations of the pending claims and/or the reasoning behind the alleged motivation to modify the cited reference has not been established.

I. The Section 103 Rejections – The Rejection of Independent Claims 1, 33 and 56

As stated above, Independent Claims 1, 33 and 56 stand rejected under 35 U.S.C. § 103 as being unpatentable over Bjorn in view of Matchett. Appellants respectfully submit that many

Attorney's Docket No. 5577-306 (RSW920010007US1)
In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001
Page 6 of 30

of the recitations of these claims are neither disclosed nor suggested by the cited references. For example, Claim 1 recites:

A system for securely providing biometric input from a user, comprising:
a security component which provides security functions, such that the security component can vouch for authenticity of one or more other components with which it the security component is securely operably connected;
a biometric sensor component that is securely operably connected, as one of the one or more other components, to the security component;
a card containing stored secrets and stored identifying information pertaining to an authorized holder of the card;
a card reader for repeatedly accessing the stored secrets and stored identifying information, wherein the stored identifying information comprises stored biometric information of the authorized holder and wherein the card reader is configured to repeatedly access the stored secrets and stored identifying information upon beginning a security-sensitive operation and is configured to terminate repeatedly accessing upon completion of the security-sensitive operation;
means for operably inserting the card into the card reader;
means for establishing a secure, operable connection between the biometric sensor, the card reader, and the security component;
means for comparing the repeatedly obtained biometric information to the stored biometric information of the authorized holder of the card; and
means for concluding, within the security component, that the security-sensitive operation is authentic based on all the one or more other components which are securely operably connected to the security component remaining securely operably connected to the security component until completion of the security-sensitive operation.

Independent Claims 33 and 56 contain corresponding computer program product and method recitations, respectively. Appellants respectfully submit that at least the highlighted portion of Claim 1 is neither disclosed nor suggested by the cited references for at least the reasons discussed herein

Paragraph 2.1 of the Response to Arguments section of the Final Office Action appears to imply that the only difference between Bjorn and Matchett is the recitation of repeatedly obtaining biometric input. See Final Office Action, pages 2-4. Furthermore, the Advisory Action confirms the implication in the Final Office Action. See Advisory Action, continuation sheet, paragraph 2. In particular, the Advisory Action states that "[t]he only difference between

Attorney's Docket No. 5577-306 (RSW920010007US1)
In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001
Page 7 of 30

Bjorn and the claimed invention is 'repeatedly' obtaining a biometric input." Appellants respectfully disagree.

As recited in Claim 1, the system includes a security component that provides security functions that can vouch for authenticity of components with which it is securely operably connected. Biometric input of a user is obtained from a biometric sensor component and stored on a card. Within a security component, the security-sensitive operation is determined to be authentic so long as the other components remain securely operably connected to the security component during the security-sensitive operation.

The specification of the present application describes the security core (security component), and authentication of components attached thereto, in accordance with some embodiments of the present invention, as follows:

In the preferred embodiments, components that authenticate themselves to the security core must remain physically attached thereto throughout an application function. Application-specific processing may be provided within each application processing subsystem to handle detachment of a component. For example, if camera module 130 is unplugged from the security core in the middle of taking a photo, the camera would have no way to transmit the photo (since it is preferably dependent on the security core for power, I/O, image storing, and so forth). If this module 130 is subsequently plugged in to a second (different) security core, that second security core would preferably stamp any pre-existing data in the camera as "unsecure" as the data traverses the second core (for example, on its way to the I/O bus of the second integrated device for purposes of storing captured images in persistent storage). (Alternatively, the second device may be adapted such that it will not accept any previously-created data.) Marking a data stream "unsecure" indicates the security core's inability to vouch for the authenticity and untampered state of I/O or application processor data.

See Specification, page 21, line 18 to page 22, line 11. In other words, the security core may conclude that a security sensitive operation with a component is not authentic if that component is disconnected, and may treat data that is later received from the reconnected component as "unsecure". Nothing in Bjorn discloses or suggests the teachings recited in Amended Claim 1.

Furthermore, Matchett does not provide the missing teaching and is not identified in the Final Office Action as providing the missing teachings. In particular, Paragraph 2.1 of the Final Office Action states:

Attorney's Docket No. 5577-306 (RSW920010007US1)
In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001
Page 8 of 30

Applicant has amended the independent claims to recite the step of "concluding that the security-sensitive operation is authentic also requires that all other components which are securely operably connected to the security core and which are involved in the security-sensitive operation remain connected until completion of the security sensitive operation". Applicant argues that this step of concluding is not taught by Bjorn. However, this added limitation is found in one of the cited art England, (column 11, line 54 through column 12, line 8)...

See Final Office Action, page 2, paragraph 2.1. Thus, it appears that the Final Office Action is pointing to England as providing the missing teachings, but does not formally reject the independent claims in view of England. See Final Office Action, page 5, illustrating the rejection of Claims 1, 33 and 56 based only on Bjorn and Matchett. Thus, Appellants submit that a proper rejection should be made over Bjorn in view of Matchett and England.

The cited portion of England recites the following:

The operating system checks the signature of a component before loading it (block 303). If the signature is valid (block 305), the component has not been compromised by someone attempting to circumvent the boot process and the process proceeds to check the level of trust assigned to the component (block 307). If the signature is not valid (or if there is no signature) but the component must be loaded (block 319), the operating system will not assume the identity of a DRAMOS upon completion of the boot process as explained further below.

A plug-and-play operating system provides an environment in which devices and their supporting software components can be added to the computer during normal operation rather than requiring all components be loaded during the boot process. If the device requires the loading of an untrusted component after the boot process completes, a plug-and-play DRAMOS must then "renounce" its trusted identity and terminate any executing trusted applications (block 323) before loading the component. The determination that an untrusted component must be loaded can be based on a system configuration parameter or on instructions from the user of the computer.

England, column 11, line 54 through column 12, line 8 (emphasis added).

The cited portion of England is a description of FIG. 3 of that reference which is shown below:

FIG. 3 of ENGLAND

Attorney's Docket No. 5577-306 (RSW920010007US1)
 In re: Doyle *et al.*
 Serial No.: 09/764,844
 Filed: January 17, 2001
 Page 9 of 30

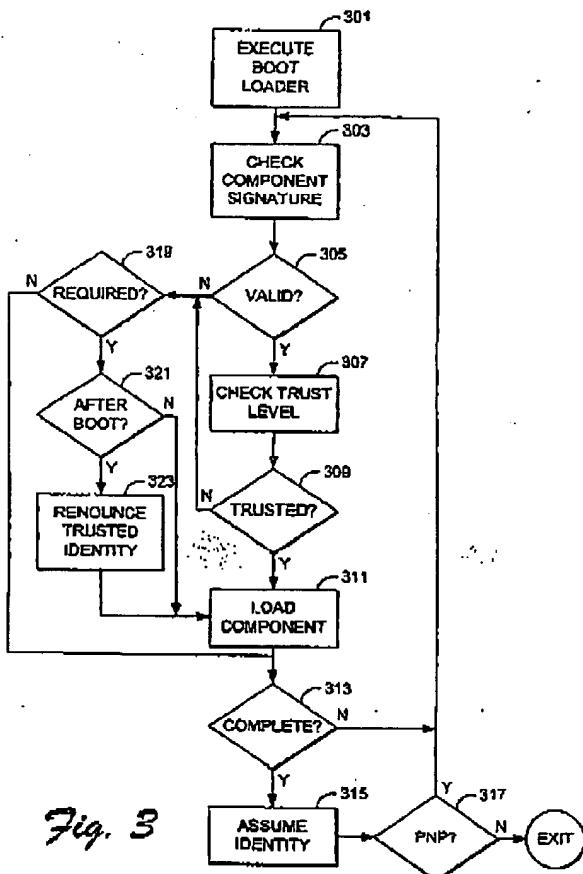


Fig. 3

With regard to FIG. 3, England describes that a component can be verified and loaded during or after a boot process. With regard to Block 303, England describes an "operating system [that] checks the signature of a component before loading it" to determine whether it is trusted or untrusted. See England, column 11, lines 54-55. England also describes that "all components are signed by a trusted source and provided with a rights manager certificate", the rights manager certificate is the signature that is checked by the operating system. See England, column 11, lines 50-51. When the signature is determined to be valid (at Blocks 305-307), the component is loaded at Block 311 into the operating system irrespective of whether the component is being loaded during the boot process or after the boot process. It is only when the signature from a component is determined at Block 305 to be invalid does the operating system

Attorney's Docket No. 5577-306 (RSW920010007US1)
In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001
Page 10 of 30

perform a further check at Block 321 as to whether the component is being tested after the boot process and, if so, then at Block 323 the operating system renounces its trust of the component

and loads the component at Block 311.

Appellants submit that nowhere does England disclose that the operating system determine whether a component is trusted or untrusted based on whether the component has remained connected to the computer. Instead, the operating system of England tests only the signature (rights manager certificate) received from the component to determine whether it is to be trusted. Consequently, once the signature (rights manager certificate) from a component is loaded into the operating system, the component can subsequently be removed from the computer and later reconnected to the computer without any effect on the determination of trustworthiness of that component by the operating system (Blocks 303-309). Accordingly, Appellants submit that the cited portion of England does not disclose or suggest at least the highlighted recitations of the independent claims for at least these reasons.

Accordingly, none of the cited references, either alone or in combination, disclose or suggest the means for concluding as recited in Claim 1. Furthermore, there is no motivation or suggestion to combine the cited references as suggested in the Final Office Action. In particular, as discussed above, the Final Office Action and the Advisory Action appear to concede that Bjorn does not disclose or suggest all of the recitations of the independent claims, namely repeatedly accessing as recited in Claim 1. See Final Office Action, page 6. However, the Final Office Action points to Matchett in an attempt to provide the missing teaching. Appellants submit that there is no motivation to combine the cited references as suggested in the Final Office Action.

As affirmed by the Court of Appeals for the Federal Circuit in *In re Sang-su Lee*, a factual question of motivation is material to patentability, and cannot be resolved on subjective belief and unknown authority. See *In re Sang-su Lee*, 277 F.3d 1338 (Fed. Cir. 2002). It is improper, in determining whether a person of ordinary skill would have been led to this

Attorney's Docket No. 5577-306 (RSW920010007US1)
In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001
Page 11 of 30

combination of references, simply to "[use] that which the inventor taught against its teacher."

W.L. Gore v. Garlock, Inc., 721 F.2d 1540, 1553, 220 U.S.P.Q. 303, 312-13 (Fed. Cir. 1983).

The Final Office Action states:

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Bjorn et al. to provide teachings means for repeatedly obtaining from the biometric sensor component biometric input of a user of the computing device and means for comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each comparison comprises an authentication of the user as taught by Matchett et al. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by Matchett et al. so as to enhance security and prevent user

substitution to an unauthorized user, for example (see column 2, lines 55-66).

See Final Office Action, page 7. This motivation is a motivation based on "subjective belief and unknown authority", the type of motivation that was rejected by the Federal Circuit in *In re Sang-su Lee*. In other words, the Final Office Action does not point to any specific portion of the cited references that would induce one of skill in the art to combine the cited references as suggested in the Final Office Action. If the motivation provided in the Final Office Action is adequate to sustain the Office's burden of motivation, then anything that would "enhance security and prevent user substitution to an unauthorized user" would render a combination obvious. This cannot be the case. Accordingly, the statement in the Final Office Action with respect to motivation does not adequately address the issue of motivation to combine as discussed in *In re Sang-su Lee*. Thus, it appears that the Final Office Action gains its alleged impetus or suggestion to combine the cited references by hindsight reasoning informed by Appellants' disclosure, which, as noted above, is an inappropriate basis for combining references.

However, for the sake of argument, even if Bjorn is combined with Matchett, they still would not disclose or suggest all of the recitations of the independent claims. Matchett states:

Security protection could be enhanced by instructing the protected system to shut down should it be disconnected from the system 400 according to the present invention. Using such connection-dependent instructions, the protected computer's keyboard could be connected through a chassis of the system 400 according to the present invention.

Attorney's Docket No. 5577-306 (RSW920010007US1)
In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001
Page 12 of 30

Matchett, Col. 10, lines 2-10. Accordingly, Matchett teaches that a protected device itself can shut down if it is disconnected from the security system. With reference to FIG. 1 of Matchett, a protected device (shown as "protected device control") can shut itself down if it is disconnected from the authentication system 100. However, Matchett does not suggest that the authentication system 100 makes any determination of authenticity of a security-sensitive operation based on the protected device becoming disconnected. Accordingly, if the protected device is reconnected to the authentication system 100, the data that is subsequently received would not be treated differently than if the protected device had not become disconnected.

Furthermore, Matchett does not teach or suggest a security core that can determine the authenticity of a security-sensitive operation based on components remaining securely operably connected to the security core during the security-sensitive operation, as recited in the independent claims. Matchett lacks such teaching because it discloses, and is concerned with, **protecting only a single protected device**. With reference to FIG. 1 of the present application, the security core of the present may protect a plurality of various different types of devices 112-136.

As a final note, the Examiner's comments in the Advisory Action contain a few statements that are not correct and Appellants would like to correct them for the record. First, paragraph 1 of the Advisory Action states:

Applicant fails to respond to more clarification and evidence presented by Examiner to maintain the rejection of Matchett and Bjorn. Applicant instead responds by saying that the final office action appears to concede that the references do not teach all the limitations by its citation for the first time of England.

See Advisory Action, continuation sheet, paragraph 1. Appellants respectfully submit that this statement is incorrect. First, nowhere in Appellants' response to the Final Office Action do Appellants say that England was cited for the first time in the Final Office Action. Appellants are aware that England was cited in the First Office Action. Second, Appellants clearly address the rejection over Bjorn and Matchett on pages 21-23 of Appellants response to the Final Office Action by discussing why one of skill in the art would not be motivated to combine Bjorn and Matchett. Furthermore, as discussed above, Appellants felt it necessary to discuss England, even

Attorney's Docket No. 5577-306 (RSW920010007US1)

In re: Doyle *et al.*

Serial No.: 09/764,844

Filed: January 17, 2001

Page 13 of 30

though no formal rejection of the independent claims was made thereon, because of the statement in paragraph 2.1 of the Final Office Action set out above.

Accordingly, for at least the reasons discussed herein, Appellants respectively submit that the *a prima facie* case of obviousness has not been established with respect to independent Claims 1, 33 and 56 as none of the cited references either alone or in combination disclose or suggest all of the recitations of these claims and there is no motivation to combine the cited references as suggested in the Final Office Action. Furthermore, the dependent claims are patentable at least per the patentability of independent Claims 1, 33 and 56 from which they depend. Thus, Appellants request reversal of the rejections of the pending claims, allowance of the pending claims and passing of the application to issue.

II. The Double Patenting Rejection

Claims 1, 33, 56 and 69 stand provisionally rejected under the nonstatutory judicially created doctrine of obviousness-type double patenting over copending U.S. Application Serial No. 09/764,827. *See* Final Office Action, page 4. Responsive to the Final Office Action, Appellants submitted a terminal disclaimer as suggested in the Final Office Action. The Advisory Action states that the Terminal Disclaimer did not comply with 37 C.F.R. § 1.321(b) and/or (c) as no fee was provided. Appellants have resubmitted the Terminal Disclaimer with the proper fee and, therefore, request withdrawal of the double patenting rejection. Copies of the originally submitted terminal disclaimer and the resubmission thereof are included herewith at Appendix B.

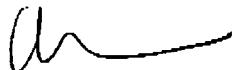
Attorney's Docket No. 5577-306 (RSW920010007US1)
In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001
Page 14 of 30

VI. Conclusion

In light of the above, Appellants request reversal of the rejections of the claims, allowance of the claims and passing of the application to issue.

It is not believed that an extension of time and/or additional fee(s) are required, beyond those that may otherwise be provided for in documents accompanying this paper. In the event, however, that an extension of time is necessary to allow consideration of this paper, such an extension is hereby petitioned for under 37 C.F.R. §1.136(a). Any additional fees believed to be due in connection with this paper may be charged to Deposit Account No. 09-0461.

Respectfully submitted,



Elizabeth A. Stanek
Registration No. 48,568

Customer No. 46589
Myers Bigel Sibley & Sajovec, P.A.
P. O. Box 37428
Raleigh, North Carolina 27627
Telephone: (919) 854-1400
Facsimile: (919) 854-1401

Attorney's Docket No. 5577-306 (RSW920010007US1)
In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001
Page 15 of 30

APPENDIX A – CLAIMS APPENDIX

1. (Previously Presented) A system for securely providing biometric input from a user, comprising:

a security component which provides security functions, such that the security component can vouch for authenticity of one or more other components with which the security component is securely operably connected;

a biometric sensor component that is securely operably connected, as one of the one or more other components, to the security component;

a card containing stored secrets and stored identifying information pertaining to an authorized holder of the card;

a card reader for repeatedly accessing the stored secrets and stored identifying information, wherein the stored identifying information comprises stored biometric information of the authorized holder and wherein the card reader is configured to repeatedly access the stored secrets and stored identifying information upon beginning a security-sensitive operation and is configured to terminate repeatedly accessing upon completion of the security-sensitive operation;

means for operably inserting the card into the card reader;

means for establishing a secure, operable connection between the biometric sensor, the card reader, and the security component;

means for comparing the repeatedly obtained biometric information to the stored biometric information of the authorized holder of the card; and

means for concluding, within the security component, that the security-sensitive operation is authentic based on all the one or more other components which are securely operably connected to the security component remaining securely operably connected to the security component until completion of the security-sensitive operation.

Claim 2 (Cancelled).

Attorney's Docket No. 5577-306 (RSW920010007US1)
In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001
Page 16 of 30

3. (Original) The system according to Claim 1, wherein selected ones of the secure operable connections are made using one or more buses of the security component.

4. (Original) The system according to Claim 1, wherein selected ones of the operable connections are made using a wireless connection between respective ones of the components and the security component.

5. (Original) The system according to Claim 4, wherein the wireless connections use Secure Sockets Layer (SSL) data encryption or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key.

6. (Original) The system according to Claim 1, wherein selected ones of the secure operable connections are provided when the security component is manufactured.

7. (Original) The system according to Claim 1, wherein the components comprise one or more of (1) input/output components and (2) application processing components.

8. (Previously Presented) The system according to Claim 1, wherein the means for establishing a secure, operable connection further comprises means for authenticating the biometric sensor and the card reader to the security component.

9. (Original) The system according to Claim 8, further comprising means for authenticating the security component to the biometric sensor and the card reader.

10. (Previously Presented) The system according to Claim 1, wherein the means for establishing a secure, operable connection is activated by a hardware reset of the one or more

Attorney's Docket No. 5577-306 (RSW920010007US1)
In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001
Page 17 of 30

components, and wherein the hardware reset is activated by the established secure, operable connection of the one or more components.

11. (Original) The system according to Claim 8, wherein the means for authenticating the biometric sensor and the card reader are securely stored thereon.

12. (Original) The system according to Claim 8, wherein the means for authenticating further comprises means for using public key cryptography.

13. (Previously Presented) The system according to Claim 1, further comprising means for concluding that the user is the authorized holder of the card only if the means for comparing succeeds.

14. (Original) The system according to Claim 1, wherein the card is a smart card.

15. (Previously Presented) The system according to Claim 1, wherein the stored secrets comprise a private key and a public key which are cryptographically related using public key cryptography, and further comprising means for digitally signing information presented to the card with the private key if the means for comparing succeeds and if the biometric sensor, the card reader, and the security component remain securely operably connected.

16. (Previously Presented) The system according to Claim 1, wherein the means for comparing is performed by the biometric sensor.

17. (Original) The system according to Claim 16, further comprising means for securely transferring the stored biometric information of the authorized holder to the biometric sensor for use by the means for comparing.

Attorney's Docket No. 5577-306 (RSW920010007US1)
In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001
Page 18 of 30

18. (Original) The system according to Claim 17, further comprising means for interrupting the secure transfer if the biometric sensor, the card reader, and the security component are no longer securely operably connected.

19. (Original) The system according to Claim 2, wherein the means for comparing is performed by the security component.

20. (Previously Presented) The system according to Claim 15, further comprising means for establishing a secure, operable connection between an application processing component and the security component, and wherein the information presented to the card is generated by the established secure, operable connected application processing component.

21. (Original) The system according to Claim 8, wherein the means for authenticating further comprises means for performing a security handshake between the biometric sensor and the security component and between the card reader and the security component.

22. (Original) The system according to Claim 21, wherein the biometric sensor and the card reader each have associated therewith: a unique device identifier that is used to identify data originating therefrom, a digital certificate, a private cryptographic key and a public cryptographic key that is cryptographically-associated with the private cryptographic key.

23. (Original) The system according to Claim 8, wherein:
the means for authenticating the biometric sensor further comprises means for using (1) a first unique identifier of the biometric sensor, (2) a first digital signature computed over the first unique identifier using a first private cryptographic key of the biometric sensor, and (3) a first public key that is cryptographically associated with the first private key; and
the means for authenticating the card reader further comprises means for using (1) a second unique identifier of the card reader, (2) a second digital signature computed over the

Attorney's Docket No. 5577-306 (RSW920010007US1)
In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001
Page 19 of 30

second unique identifier using a second private cryptographic key of the card reader, and (3) a second public key that is cryptographically associated with the second private key.

Claims 24-32 (Cancelled).

33. (Previously Presented) A computer program product for securely providing biometric input from a user, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code configured to operate a security component which provides security functions, such that the security component can vouch for authenticity of one or more other components with which the security component is securely operably connected;

computer-readable program code configured to operate a biometric sensor that is securely, operably connected, as one of the one or more other components, to the security component;

computer-readable program code configured to access a card containing stored secrets and stored identifying information pertaining to an authorized holder of the card;

computer-readable program code configured to operate a card reader for repeatedly accessing the stored secrets and stored identifying information, wherein the stored identifying information comprises stored biometric information of the authorized holder and wherein the card reader is configured to repeatedly access the stored secrets and stored identifying information upon beginning a security-sensitive operation and is configured to terminate repeatedly accessing upon completion of the security-sensitive operation;

computer-readable program code configured to detect and respond to an operable insertion of the card into the card reader;

computer-readable program code configured to establish a secure, operable connection between the biometric sensor, the card reader, and the security component;

Attorney's Docket No. 5577-306 (RSW920010007US1)
In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001
Page 20 of 30

computer readable program code configured to compare the repeatedly obtained biometric information to the stored biometric information of the authorized holder of the card; and

computer readable program code configured to conclude, within the security component, that the security-sensitive operation is authentic based on all the one or more other components which are securely operably connected to the security component remaining securely operably connected to the security component until completion of the security-sensitive operation.

Claim 34 (Cancelled).

35. (Original) The computer program product according to Claim 33, wherein selected ones of the secure operable connections are made using one or more buses of the security component.

36. (Original) The computer program product according to Claim 33, wherein selected ones of the operable connections are made using a wireless connection between respective ones of the components and the security component.

37. (Original) The computer program product according to Claim 36, wherein the wireless connections use Secure Sockets Layer (SSL) data encryption or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key.

38. (Original) The computer program product according to Claim 33, wherein selected ones of the secure operable connections are provided when the security component is manufactured.

Attorney's Docket No. 5577-306 (RSW920010007US1)
In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001
Page 21 of 30

39. (Original) The computer program product according to Claim 33, wherein the components comprise one or more of (1) input/output components and (2) application processing components.

40. (Previously Presented) The computer program product according to Claim 33, wherein the computer-readable program code configured to establish a secure, operation connection further comprises computer-readable program code configured to authenticate the biometric sensor and the card reader to the security component.

41. (Previously Presented) The computer program product according to Claim 40, further comprising computer-readable program code configured to authenticate the security component to the biometric sensor and the card reader.

42. (Previously Presented) The computer program product according to Claim 33, wherein the computer-readable program code configured to establish a secure, operable connection is activated by a hardware reset of the one or more components, and wherein the hardware reset is activated by the established secure, operable connection of the one or more components.

43. (Previously Presented) The computer program product according to Claim 40, wherein the computer-readable program code configured to authenticate the biometric sensor and the card reader are securely stored thereon.

44. (Previously Presented) The computer program product according to Claim 40, wherein the computer-readable program code configured to authenticate further comprises computer-readable program code configured to use public key cryptography.

Attorney's Docket No. 5577-306 (RSW920010007US1)
In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001
Page 22 of 30

45. (Previously Presented) The computer program product according to Claim 33, further comprising computer- readable program code configured to conclude that the user is the authorized holder of the card only if the means for comparing succeeds.

46. (Original) The computer program product according to Claim 33, wherein the card is a smart card.

47. (Previously Presented) The computer program product according to Claim 33, wherein the stored secrets comprise a private key and a public key which are cryptographically related using public key cryptography, and further comprising computer-readable program code configured to digitally sign information presented to the card with the private key if the computer-readable program code configured to compare succeeds and if the biometric sensor, the card reader, and the security component remain securely operably connected.

48. (Previously Presented) The computer program product according to Claim 33, wherein the computer-readable program code configured to compare is performed by the biometric sensor.

49. (Previously Presented) The computer program product according to Claim 48, further comprising computer- readable program code configured to securely transfer the stored biometric information of the authorized holder to the biometric sensor for use by the computer- readable program code configured to compare.

50. (Previously Presented) The computer program product according to Claim 49, further comprising computer- readable program code configured to interrupt the secure transfer if the biometric sensor, the card reader, and the security component are no longer securely operably connected.

Attorney's Docket No. 5577-306 (RSW920010007US1)
In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001
Page 23 of 30

51. (Previously Presented) The computer program product according to Claim 33, wherein the computer-readable program code configured to compare is performed by the security component.

52. (Previously Presented) The computer program product according to Claim 47, further comprising computer- readable program code configured to establish a secure, operable connection between an application processing component and the security component, and wherein the information presented to the card is generated by the connected application processing component.

53. (Previously Presented) The computer program product according to Claim 40, wherein the computer-readable program code configured to authenticate further comprises computer-readable program code configured to perform a security handshake between the biometric sensor and the security component and between the card reader and the security component.

54. (Original) The computer program product according to Claim 53, wherein the biometric sensor and the card reader each have associated therewith: a unique device identifier that is used to identify data originating therefrom, a digital certificate, a private cryptographic key and a public cryptographic key that is cryptographically-associated with the private cryptographic key.

55. (Previously Presented) The computer program product according to Claim 40, wherein:

the computer-readable program code configured to authenticate the biometric sensor further comprises computer-readable program code configured to use (1) a first unique identifier of the biometric sensor, (2) a first digital signature computed over the first unique identifier using

Attorney's Docket No. 5577-306 (RSW920010007US1)
In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001
Page 24 of 30

a first private cryptographic key of the biometric sensor, and (3) a first public key that is cryptographically associated with the first private key; and

the computer-readable program code configured to authenticate the card reader further comprises computer-readable program code configured to use (1) a second unique identifier of the card reader, (2) a second digital signature computed over the second unique identifier using a second private cryptographic key of the card reader, and (3) a second public key that is cryptographically associated with the second private key.

56. (Previously Presented) A method of securely providing biometric input from a user, comprising:

operating a security component which provides security functions, such that the security component can vouch for authenticity of one or more other components with which the security component is securely operably connected;

operating a biometric sensor component that is securely, operably connected, as one of the one or more other components, to the security component;

accessing a card containing stored secrets and stored identifying information pertaining to an authorized holder of the card;

operating a card reader for repeatedly accessing the stored secrets and stored identifying information, wherein the stored identifying information comprises stored biometric information of the authorized holder and wherein the card reader is configured to repeatedly access the stored secrets and stored identifying information upon beginning a security-sensitive operation and is configured to terminate repeatedly accessing upon completion of the security-sensitive operation;

detecting and responding to an operable insertion of the card into the card reader;

establishing a secure, operable connection the biometric sensor, the card reader, and the security component;

comparing the repeatedly obtained biometric information to the stored biometric information of the authorized holder of the card; and concluding, within the security component, that the security-sensitive operation is authentic based on all the one or more other

Attorney's Docket No. 5577-306 (RSW920010007US1)
In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001
Page 25 of 30

components which are securely operably connected to the security component remaining securely operably connected to the security component until completion of the security-sensitive operation.

Claim 57 (Cancelled).

58. (Original) The method according to Claim 56, wherein selected ones of the secure operable connections are made using one or more buses of the security component.

59. (Original) The method according to Claim 56, wherein selected ones of the operable connections are made using a wireless connection between respective ones of the components and the security component.

60. (Original) The method according to Claim 59, wherein the wireless connections use Secure Sockets Layer (SSL) data encryption or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key.

61. (Original) The method according to Claim 56, wherein selected ones of the secure operable connections are provided when the security component is manufactured.

62. (Original) The method according to Claim 56, wherein the components comprise one or more of (1) input/output components and (2) application processing components.

63. (Previously Presented) The method according to Claim 56, wherein establishing a secure, operable connection further comprises authenticating the biometric sensor and the card reader to the security component.

Attorney's Docket No. 5577-306 (RSW920010007US1)
In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001
Page 26 of 30

64. (Previously Presented) The method according to Claim 63, further comprising authenticating the security component to the biometric sensor and the card reader.

65. (Previously Presented) The method according to Claim 56, wherein establishing a secure, operable connection is activated by a hardware reset of the one or more components, and wherein the hardware reset is activated by the established secure, operable connection of the one or more components.

66. (Original) The method according to Claim 63, wherein instructions for authenticating the biometric sensor and the card reader are securely stored thereon.

67. (Previously Presented) The method according to Claim 63, wherein authenticating further comprises using public key cryptography.

68. (Previously Presented) The method according to Claim 56, further comprising concluding that the user is the authorized holder of the card only if comparing succeeds.

69. (Original) The method according to Claim 56, wherein the card is a smart card.

70. (Previously Presented) The method according to Claim 56, wherein the stored secrets comprise a private key and a public key which are cryptographically related using public key cryptography, and further comprising digitally signing information presented to the card with the private key if comparing succeeds and if the biometric sensor, the card reader, and the security component remain securely operably connected.

Attorney's Docket No. 5577-306 (RSW920010007US1)
In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001
Page 27 of 30

71. (Previously Presented) The method according to Claim 56, wherein comparing is performed by the biometric sensor.

72. (Previously Presented) The method according to Claim 71, further comprising securely transferring the stored biometric information of the authorized holder to the biometric sensor for use comparing.

73. (Previously Presented) The method according to Claim 72, further comprising interrupting the secure transfer if the biometric sensor, the card reader, and the security component are no longer securely operably connected.

74. (Previously Presented) The method according to Claim 56, wherein comparing is performed by the security component.

75. (Previously Presented) The method according to Claim 70, further comprising establishing a secure, operable connection an application processing component to the security component, and wherein the information presented to the card is generated by the securely operably connected application processing component.

76. (Previously Presented) The method according to Claim 63, wherein authenticating further comprises performing a security handshake between the biometric sensor and the security component and between the card reader and the security component.

77. (Original) The method according to Claim 76, wherein the biometric sensor and the card reader each have associated therewith: a unique device identifier that is used to identify data originating therefrom, a digital certificate, a private cryptographic key and a public cryptographic key that is cryptographically-associated with the private cryptographic key.

78. (Previously Presented) The method according to Claim 63, wherein:

Attorney's Docket No. 5577-306 (RSW920010007US1)
In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001
Page 28 of 30

authenticating the biometric sensor further comprises using (1) a first unique identifier of the biometric sensor, (2) a first digital signature computed over the first unique identifier using a first private cryptographic key of the biometric sensor, and (3) a first public key that is cryptographically associated with the first private key; and

authenticating the card reader further comprises using (1) a second unique identifier of the card reader, (2) a second digital signature computed over the second unique identifier using a second private cryptographic key of the card reader, and (3) a second public key that is cryptographically associated with the second private key.

APPENDIX B – EVIDENCE APPENDIX

- I. Terminal Disclaimer submitted on May 2, 2005 (copy attached hereto)
- II. Resubmission of Terminal Disclaimer with fee submitted concurrently herewith (copy attached hereto)

**RESPONSE UNDER 37 C.F.R. 1.116 - EXPEDITED
PROCEDURE - EXAMINING GROUP 2136**

Attorney's Docket No. 5577-306

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001
For: SMART CARD WITH INTEGRATED BIOMETRIC SENSOR

COPY

Confirmation No.: 6508

Group No.: 2136

Examiner: Carl G. Colin

Date: May 2, 2005

Mail Stop AF
Commissioner for Patents
Box 1450
Alexandria, VA 22313-1450

Certificate of Facsimile Transmission
I hereby certify that this correspondence is being
transmitted by facsimile to the U.S. Patent and Trademark
Office on May 2, 2005 via facsimile number 703-872-9306.

Gin A. Campion

TERMINAL DISCLAIMER UNDER 37 C.F.R. 1.321

Sir:

I, Elizabeth A. Stanek, am an attorney of record of the owner and disclaimant, International Business Machines Corporation and am authorized to execute this Terminal Disclaimer on behalf thereof. International Business Machines Corporation is the owner of all right, title, and interest in the above-identified application as evidenced by an Assignment recorded on January 17, 2001, at Reel 011487, Frame 0222.

The owner, International Business Machines Corporation of the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending U.S. Patent Application Serial Number 09/764,827, filed on January 17, 2001, as such term is defined in 35 U.S.C. §§154 – 156, §173, and any other relevant statutory provision, and as the term of any patent granted on U.S. Patent Application Serial Number 09/764,827 may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending U.S. Patent Application Serial Number 09/764,827. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on U.S. Patent Application Serial Number 09/764,827 are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001

COPY

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term as defined in U.S.C. §§154 – 156, §173, and any other relevant statutory provision, of any patent granted on U.S. Patent Application Serial Number 09/764,827 as the term of any patent granted on U.S. Patent Application Serial Number 09/764,827 may be shortened by any terminal disclaimer filed prior to the grant of any patent on U.S. Patent Application Serial Number 09/764,827, in the event that any such patent granted on pending U.S. Patent Application Serial Number 09/764,827: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR §1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

Respectfully submitted,



Elizabeth A. Stanek
Registration No. 48,568

USPTO Customer No. 46589
Myers Bigel Sibley & Sajovec
Post Office Box 37428
Raleigh, North Carolina 27627
Telephone: 919/854-1400
Facsimile: 919/854-1401

Attorney's Docket No. 5577-306

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001
For: SMART CARD WITH INTEGRATED BIOMETRIC SENSOR

Confirmation No.: 6508
Group No.: 2136
Examiner: Carl G. Colin

COPY

Date: August 5, 2005

Mail Stop AF
Commissioner for Patents
Box 1450
Alexandria, VA 22313-1450

Certificate of Facsimile Transmission
I hereby certify that this correspondence is being transmitted
by facsimile to the U.S. Patent and Trademark Office on
August 5, 2005 via facsimile number 571-273-8300.


Traci A. Brown**RESUBMISSION OF TERMINAL DISCLAIMER
UNDER 37 C.F.R. § 1.321(b)**

Sir:

Applicant hereby resubmits the enclosed Terminal Disclaimer Under 37 C.F.R. § 1.321 for the above referenced application responsive to the Advisory Action of May 26, 2005. The Examiner objected to the previous submission as lacking the required fee. The Examiner is authorized to charge Deposit Account No. 09-0461 in the amount of \$110.00 [37 C.F.R. § 1.20(d)] to cover the fee for filing a Terminal Disclaimer and for any additional fee which may be required or to credit any overpayment.

Respectfully submitted,


Elizabeth A. Stanek
Registration No. 48,568

USPTO Customer No. 46589
Myers Bigel Sibley & Sajovec
Post Office Box 37428
Raleigh, North Carolina 27627
Telephone: 919/854-1400
Facsimile: 919/854-1401

Attorney's Docket No. 5577-306

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001
For: SMART CARD WITH INTEGRATED BIOMETRIC SENSOR

COPY Confirmation No.: 6508

Group No.: 2136

Examiner: Carl G. Colin

In re: Doyle *et al.*
Serial No.: 09/764,844
Filed: January 17, 2001

COPY

patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term as defined in U.S.C. §§154 – 156, §173, and any other relevant statutory provision, of any patent granted on U.S. Patent Application Serial Number 09/764,827 as the term of any patent granted on U.S. Patent Application Serial Number 09/764,827 may be shortened by any terminal disclaimer filed prior to the grant of any patent on U.S. Patent Application Serial Number 09/764,827, in the event that any such patent granted on pending U.S. Patent Application Serial Number 09/764,827: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR §1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

Respectfully submitted,



Elizabeth A. Stanek
Registration No. 48,568

USPTO Customer No. 46589
Myers Bigel Sibley & Sajovec
Post Office Box 37428
Raleigh, North Carolina 27627
Telephone: 919/854-1400
Facsimile: 919/854-1401

AUG. 5. 2005 5:27PM 919-854-1401 MBS&S

NO. 8480 P. 36

APPENDIX C – RELATED PROCEEDINGS

(NONE)